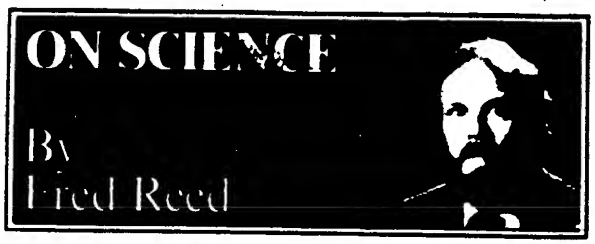
ARTICLE APPEARED
ON PAGE 2-A

WASHINGTON TIMES
16 July 1985

National



High-tech snoops drive you buggy

Oh boy: Spying, mystery. The secret agent in a cloak, waving his dagger and, down a dark foggy alley in London, peering at his oscilloscope. Espionage has gone technological, like everything else. In the July issue of Spectrum I found a long article about it.

It seems that companies are worried about electronic spying — i.e. having their proprietary secrets picked off by snoopers from other firms. Inevitably lots of little companies have sprung up alleging to prevent this and, at least as inevitably, they are making the threat seem worse than it is. Anyway, some of the techniques:

Says Spectrum, the closer the listener is to his victim, the cheaper it is to spy. A telephone in the target's office can easily be modified to remain "off-hook" so that the snooper can listen to whatever is going on in the room from another telephone. Of course you have to be able to get into the office. Or you can plant a microphone and FM transmitter. This will cost you $50 to $150.

Interesting, although obviously if you think about how a loudspeaker works, a speaker already in the target's office can be used for a microphone.

At a greater distance, you can tap into the telephone lines beyond the target's immediate loop. This will cost you six grand, but you should get admiring glances at your trial for your ingenuity.

Or you can try to get the target's calls by listening in on microwave relays — those funny towers that have what look like lots of garbage-can lids on them. This will set you back 40 grand in electronics, but it is a tony, up-scale thing to do. Hide your dish antennas in a barn.

By the way, if you want to see some fancy antenna farms used for this kind of thing, among many others, check out the roofs of a few embassies. Note the high ground on which the new Soviet embassy sits. What idiot was responsible for this? Statistically, a good guess is the largest concentration of idiots in town, the State Department . . .

OK, the foregoing are some of the ways to snoop. How do you sweep an office to get rid of bugs and taps? With difficulty. With great difficulty.

The problem is that the advantage lies with the spy. Devices hidden in an office can be very small. Finding them, particularly if they are behind walls, isn't easy. If the device is a transmitter, finding it when it is off is a chore. If the spy is listening to microwave relays, well, he's got enough money and knowledge that you are never going to feel really secure. And any good engineer can come up with a thousand ingenious techniques for making a sweep difficult.

Example: I read recently (if memory serves) that the Soviets managed to hide pick-ups in the Selectric typewriters in the U.S. embassy in Moscow. How they did this is a question someone isn't going to want to answer. Anyway, the ball takes differing amounts of time to spin to different letters, so if you have a computer . . . yep.

There are cute counter-gadgets that work sometime. For example, with a time-domain reflectometer (my cocktail buzz-word for this week) you send a signal down a line you think is tapped, and get reflections from rough spots in the line — splices, for example.

Another gizzwhich called a non-linear junction detector picks up the harmonics produced when its own signal encounters a transistor (or, alas, hinges, or nails driven through metal studs, or . . . well, you can tear out a lot of walls for nothing.) In short, judging by Spectrum, it's hard to be sure. It's a fun subject so I'll go look into it and report.

So if you really want secure communications, you have to go to encryption. If you can encode your data or conversations well enough, it may not make any difference whether the bad guy intercepts them. Encryption is another fun subject. We'll get to it before long.